

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF INDIANA**

ELIZABETH FURCINITO and MIRIAM  
BARNICLE, individually and on behalf of all  
others similarly situated,

Plaintiffs,

V.

HERFF JONES, LLC,

Defendant.

Case No. 1:21-cv-01661

# CLASS ACTION COMPLAINT

## JURY TRIAL DEMANDED

Plaintiffs Elizabeth Furcinito and Miriam Barnicle (“Plaintiffs”), individually and on behalf of all others similarly situated, allege the following against Defendant Herff Jones, LLC (“Herff Jones” or “Defendant”) to obtain damages, restitution, and injunctive relief for the Class, based on personal knowledge as to their own experiences and upon information and belief on investigation of counsel as to all other matters.

## NATURE OF THE ACTION

1. Plaintiffs bring this action, individually and on behalf of all others similarly situated whose personal and non-public information – including on information and belief, credit card and debit card numbers, expiration dates, cardholder names, and other payment card information (collectively, “Card Information”) – was compromised in a security breach of Herff Jones’s computer servers (the “Data Breach”).

2. In early May 2021, news reports began surfacing that Herff Jones—a company that is well known for selling and renting graduation products—was subject to a data breach impacting student bodies from numerous colleges and universities. Details about the scope and magnitude of

the breach are not yet available, but reports indicate that students from numerous schools partnering with Herff Jones for graduation-related needs have suffered fraudulent charges following their transactions with Herff Jones, and that Herff Jones has begun notifying impacted universities of the Data Breach.<sup>1</sup>

3. As a result of the Data Breach, many thousands of consumers—mainly graduates and their parents—have had their sensitive Card Information exposed to fraudsters resulting from purchases made through Herff Jones, including purchases and rentals of graduation caps, gowns, rings, announcements, and other products.

4. In its website statement concerning the Data Breach, Herff Jones claims it is “committed to the privacy and security of its customers,” but as alleged herein, Herff Jones utterly failed to implement adequate data security measures to protect its customers’ sensitive Card Information, directly and proximately causing injuries to Plaintiffs and the class.

5. The Data Breach was the inevitable result of Herff Jones’s inadequate data security measures and cavalier approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving payment card networks and systems, and the fact that these types of data breaches occur frequently throughout the retail industry, Herff Jones failed to ensure that it maintained adequate data security measures to protect customer Card Information from criminals.

6. As a direct and proximate consequence of Herff Jones’s conduct and data security failings, a massive amount of sensitive customer Card Information was stolen from Herff Jones and exposed to criminals. That Plaintiffs and so many other consumers are reporting multitudinous

---

<sup>1</sup> Haya Panjwani, *Herff Jones data breach leaves students’ bank information compromised*, THE COUGAR (May 10, 2021), <http://thedailycougar.com/2021/05/10/herff-jones-breach-bank-information/>.

fraudulent charges following their Herff Jones purchases makes clear that the criminals who stole the Card Information are acting quickly to monetize that information.

7. Herff Jones publicly acknowledged the Data Breach on or about May 12, 2021, but has remained silent as to the exact number of individuals whose Card Information was compromised, the window of time of the Data Breach, the list of universities impacted, and other important information that would allow breach victims to take steps to secure their sensitive information—thus leaving victims in the dark.

8. Plaintiffs and other victims of the Data Breach have had their sensitive Card Information compromised, their privacy rights violated, suffered actual fraud, been exposed to the increased risk of fraud and identity theft, lost control over their personal and financial information, and been otherwise injured.

9. Moreover, Plaintiffs and class members have been forced to spend significant time associated with addressing the fallout of the Data Breach, including, among other things, closing out and opening new credit or debit card accounts, ordering replacement cards, obtaining fraud monitoring services, communicating with banks, losing access to cash flow and credit lines, monitoring credit reports and accounts, and/or other losses resulting from unauthorized use of their cards or accounts.

10. Based upon numerous reports of actual fraud suffered by breach victims, on information and belief, the stolen sensitive Card Information is already available for illegal purchase on the dark web or is otherwise being utilized by criminals to commit fraud.

11. Rather than providing meaningful assistance or direction to consumers to help deal with the fraud that has and will continue to result from the Data Breach, Herff Jones's dedicated website for the Data Breach merely states, "[w]e sincerely apologize to those impacted by this

incident,” and requests that people call Herff Jones if they believe they have been impacted by the Data Breach.<sup>2</sup>

12. In short, Herff Jones has placed the onus squarely on its customers to deal with the negative repercussions of the Data Breach. Contrasting what has been frequently made available to consumers in other data breaches, on information and belief, Herff Jones has not publicly offered or provided any credit monitoring service or fraud insurance to victims of the Data Breach.

13. Plaintiffs and class members seek to recover damages caused by Herff Jones’s negligence, negligence per se, breach of contract, and violations of state consumer protection statutes. Additionally, Plaintiffs seek declaratory and injunctive relief as a result of the conduct discussed herein.

### **PARTIES**

#### **Plaintiff Miriam Barnicle**

14. Plaintiff Miriam Barnicle is an adult residing in Milwaukee, Wisconsin. On April 20, 2021, Plaintiff used her Discover credit card to make a purchase with Herff Jones for approximately \$8.39 to pay for the shipping costs associated with the cap and gown for her graduation from Alverno College.

15. Following her purchase with Herff Jones, on May 17, 2021, a fraudulent charge was made on Plaintiff Barnicle’s Discover card. Specifically, a criminal used her card to make seven unauthorized fraudulent charges with Printify totaling approximately \$112. Plaintiff Barnicle has experienced actual fraud as a result of the Data Breach.

16. As a result, Plaintiff Barnicle was forced to call Discover to report the fraudulent charges, and was informed that Discover is conducting an ongoing investigation of the fraud.

---

<sup>2</sup> Press Release, Herff Jones, Herff Jones Cyber Security Incident Update (May 12, 2021), <http://content.herffjones.com/about/press-releases/herff-jones-cyber-security-incident-update/>.

17. Plaintiff Barnicle subsequently received an e-mail from Alverno College informing her that students or parents who shopped at Herff Jones may have been exposed to the Data Breach.

18. Plaintiff Barnicle then called Herff Jones, provided her name and address to an employee of Herff Jones, and was informed by Herff Jones that her identity was compromised. During the call, Herff Jones told her that she should contact her bank, and it would not confirm whether her sensitive information remains at risk. Herff Jones did not do anything to assist her with the impact of the Data Breach.

19. Prior to learning that her payment card was impacted by the Data Breach, Plaintiff Barnicle had never experienced fraudulent charges on or identity theft with respect to her Discover card.

20. As a result of having been victimized by the Data Breach, Plaintiff Barnicle was required to spend a significant amount—approximately three hours—addressing the fraud concerns related to her compromised card. To date, Herff Jones has not offered her any credit monitoring or other similar services.

21. At the time she made her purchase at Herff Jones, Plaintiff Barnicle believed that Herff Jones provided secure services and would protect and keep secure her Card Information that she provided during the transaction. Had she known that Herff Jones would not adequately protect her Card Information and other sensitive information she entrusted to it, she would not have made a purchase at Herff Jones using her payment card.

22. As a result of Herff Jones's failure to adequately safeguard Plaintiff's Card Information, Plaintiff Barnicle has been injured.

**Plaintiff Elizabeth Furcinito**

23. Plaintiff Elizabeth Furcinito is an adult residing in Liverpool, New York. On March 30, 2021, Plaintiff used her Apple credit card (“Apple Card”) to make a purchase with Herff Jones in the amount of \$8.59 to pay for the shipping costs associated with her cap and gown for her graduation from Syracuse University.

24. Following her purchase with Herff Jones, on May 19, 2021 a fraudulent charge was made on Plaintiff Furcinito’s Apple Card. Specifically, a criminal used her card to make an unauthorized fraudulent charge at a Best Buy store located in El Paso, Texas in the amount of \$2,995.99. Plaintiff Furcinito has experienced actual fraud as a result of the Data Breach.

25. Plaintiff Furcinito subsequently communicated with Apple via its support messaging system about the fraudulent charge and as a result, was given a new card number for her Apple Card. Plaintiff also spent time checking other her bank accounts and transactions, and had to review various account statements to determine if she suffered any additional fraudulent charges.

26. Prior to learning that her payment card was impacted by the Data Breach, Plaintiff Furcinito had never experienced fraudulent charges on or identity theft with respect to her Apple Card.

27. As a result of being victimized by the Data Breach, Plaintiff Furcinito was required to spend a significant amount of time—approximately three hours—addressing the fraud concerns related to her compromised Apple Card.

28. At the time she made her purchase at Herff Jones, Plaintiff Furcinito believed that Herff Jones provided secure services and would protect and keep secure the Card Information that she provided during the transaction. Had Plaintiff Furcinito known that Herff Jones would not

adequately protect her Card Information and other sensitive information entrusted to it, she would not have made a purchase at Herff Jones using her payment card.

29. As a result of Herff Jones's failure to adequately safeguard Plaintiff's Card Information, Plaintiff Furcinito has been injured.

**Defendant Herff Jones, LLC**

30. Defendant Herff Jones, LLC is an Indiana corporation that maintains its principal place of business at 4625 West 62nd Street, Indianapolis, Indiana, 46268. Herff Jones is a brand or subsidiary of Bain Capital-owned Varsity Brands.

31. Herff Jones manufactures and sells educational recognition and achievement products, including graduation caps, gowns, rings, and other commemorative graduation products. Per its website, Herff Jones maintains manufacturing facilities across the United States, and it transacts business throughout the United States through its website and affiliated representatives.

**JURISDICTION AND VENUE**

32. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds \$5 million, exclusive of interest and costs, and is a class action in which some members of the class are citizens of states different than Herff Jones. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

33. This Court has personal jurisdiction over Herff Jones. Herff Jones has sufficient minimum contacts with the state of Indiana—including maintaining a principal place of business and conducting substantial business in Indiana—and it intentionally avails itself of the consumers and markets within the state through the promotion, marketing, and sale of its products and services.

34. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(1) because Herff Jones resides in the district. Likewise, a substantial part of the events and/or omissions giving rise to the claims occurred within this district. *See* 28 U.S.C. § 1391(a)(2).

### **FACTUAL ALLEGATIONS**

#### **The Herff Jones Data Breach**

35. On or about May 12, 2021, Herff Jones confirmed in a “Cyber Security Incident Update” (the “Update”) posted on its website that it had been made aware of a possible data breach compromising its customers’ sensitive Card Information. The Update provides the following:

May 12, 2021

#### **HERFF JONES CYBER SECURITY INCIDENT UPDATE**

Herff Jones recently became aware of suspicious activity involving certain customers’ payment card information. We promptly launched an investigation and engaged a leading cybersecurity firm to assist in assessing the scope of the incident. We have taken steps to mitigate the potential impact and notified law enforcement. Herff Jones is committed to the privacy and security of its customers and we take this responsibility seriously.

During the course of our investigation, which is ongoing, we identified theft of certain customers’ payment information.

We sincerely apologize to those impacted by this incident. We are working diligently to identify and notify impacted customers. In the meantime, we have a dedicated customer service team that can be reached by calling 855-535-1795 between 9 a.m. and 9 p.m. EDT Monday through Friday.<sup>3</sup>

36. To date, Herff Jones does not appear to have disclosed any additional specifics about the Data Breach, including the number of individuals impacted, the number of universities impacted, the duration of the Data Breach, and the nature of the breach (*e.g.*, malware, ransomware).

---

<sup>3</sup> Press Release, Herff Jones, Herff Jones Cyber Security Incident Update (May 12, 2021), <http://content.herffjones.com/about/press-releases/herff-jones-cyber-security-incident-update/>.

37. To date, individuals impacted by the Data Breach have received no direct notice from Herff Jones regarding the Data Breach. Many individuals learned about the breach when they learned that their payment cards were used to make fraudulent charges. In other instances, universities impacted by the Data Breach have been informed by Herff Jones that their students are impacted, and university officials then passed this information along to the student population.

38. On information and belief, despite having contact information for its customers, Herff Jones is providing no targeted notice to impacted class members and is not identifying to universities the students who have been victimized by the Data Breach. As a result, the universities send general notifications to the student populations at affected campuses, leaving students in the dark and requiring them to take steps to determine whether they have been impacted.

39. Based on the most recent reports and the investigation of counsel, the list of schools impacted by the Data Breach includes at least the following: Purdue University, University of Houston, University of Illinois, University of Delaware, George Washington University, Towson University, Bradley University, Alverno College, the University of Southern California, Wake Forest University, Millikin University, Boston University, and Cornell University.

40. Herff Jones has ready capacity to directly notify impacted class members about the Data Breach. Indeed, as part of the process of placing a purchase with Herff Jones, class members are required to provide the following information: names, billing addresses, delivery addresses, email addresses, and telephone numbers. However, Herff Jones decided against this most efficient and beneficial form of notifying Data Breach victims.

41. Likewise, class members are also required to provide other information as part of placing a purchase with Herff Jones, including: card type, name on card, card number, card expiration date, and security or CVV code.

42. While Herff Jones has not confirmed the exact credit and debit card information exposed during the Data Breach, Herff Jones collects and stores the foregoing, comprehensive information. Thus, the numerous reports of Herff Jones' customers suffering fraudulent charges raises the probability that its customers' credit and debit card information was stolen in the Data Breach.

43. Neither the Update nor any statements issued by Herff Jones give any indication of the actual magnitude of the Data Breach. No confirmation has been provided of the targeted universities or schools targeted or the actual number of customers and cards affected.

44. While Herff Jones claims in the Update that it "is committed to the privacy and security of its customers," Herff Jones has provided next to nothing by way of details surrounding the breach that would allow consumers to protect themselves against payment card fraud and identity theft.

45. Although the Update indicates Herff Jones "notified law enforcement," it is unclear whether Herff Jones has reported the full details of the Data Breach to the appropriate law enforcement, and whether Herff Jones acted timely in providing all impacted victims with notice of the Data Breach.

#### **Industry Standards and the Protection of Customer Card Information**

46. It is well known that sensitive Card Information is valuable and frequently targeted by hackers. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in payment systems either online or in stores."<sup>4</sup>

---

<sup>4</sup> Dennis Green and Mary Hanbury, *If you bought anything from these 11 companies in the last year, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019), <https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1>.

47. Despite the known risk of a data breach and the widespread publicity and industry alerts regarding other notable data breaches, Herff Jones failed to take reasonable steps to adequately protect its systems from being breached.

48. Herff Jones is, and at all relevant times has been, aware that the Card Information it maintains as a result of purchases made by its customers is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases. On its website, Herff Jones discloses a robust Privacy Policy in which it states that it may collect the following information as part of a purchase:

The information you provide directly to us includes, but is not limited to: (i) name; (ii) email address; (iii) age; (iv) postal address; (v) username and password associated with your account; (vi) phone numbers; (vi) measurements for uniform orders; and (viii) demographic information. If you order a product or service that we offer for sale through the Services, we may also collect and maintain your billing address, shipping address, product selections, financial information (such as your credit or debit card information or ACH information, applicable card expiration dates and security codes) and your order number.<sup>5</sup>

49. Herff Jones's Privacy Policy demonstrates its awareness of the importance of safeguarding its customers' Card Information from the foreseeable consequences from a breach of its data security systems.

50. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure that consumers' valuable data is protected.

51. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where

---

<sup>5</sup> *Varsity Brands Privacy Policy*, HERFF JONES (Dec. 30, 2019), <https://www.herffjones.com/about/privacy/#info>.

cardholder data is stored, processed, or transmitted, and requires merchants like Herff Jones to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

52. The twelve requirements of the PCI DSS are: (1) Install and maintain a firewall configuration to protect cardholder data; (2) Do not use vendor-supplied defaults for system passwords and other security parameters; (3) Protect stored cardholder data; (4) Encrypt transmission of cardholder data across open, public networks; (5) Protect all systems against malware and regularly update anti-virus software or programs; (6) Develop and maintain secure systems and applications; (7) Restrict access to cardholder data by business need to know; (8) Identify and authenticate access to system components; (9) Restrict physical access to cardholder data; (10) Track and monitor all access to network resources and cardholder data; (11) Regularly test security systems and processes; (12) Maintain a policy that addresses information security for all personnel.<sup>6</sup>

53. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

54. Herff Jones was, at all material times, fully aware of its data protection obligations in light of its participation in the payment card processing networks and its daily collection and transmission of many thousands of sets of Card Information.

---

<sup>6</sup> *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard Version 3.2.1* at 9, PCI SECURITY STANDARDS COUNCIL, (July 2018), [https://www.pcisecuritystandards.org/documents/PCI\\_DSS-QRG-v3\\_2\\_1.pdf?agreement=true&time=1623090670910](https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1623090670910).

55. Because Herff Jones accepted payment cards containing sensitive financial information, it knew that its customers were entitled to, and did in fact, rely on it to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

56. Additionally, according to the Federal Trade Commission (“FTC”), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 (“FTC Act”), 15 U.S.C. § 45.

57. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

58. The FTC has also published a document, entitled “Protecting Personal Information: A Guide for Business,” which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.<sup>7</sup>

---

<sup>7</sup> *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION, (Oct. 2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).

59. The FTC has issued orders against businesses that failed to employ reasonable measures to secure payment card data. These orders provide further guidance to businesses with regards to their data security obligations.

60. As noted above, Herff Jones was or should have been aware of the need to have adequate data security systems in place.

61. Despite this, Herff Jones failed to maintain its data security systems in a meaningful way in order prevent data breaches. Herff Jones's security flaws run afoul of industry best practices and standards. More specifically, the security practices in place at Herff Jones are in stark contrast and directly conflict with the PCI DSS core security standards.

62. Had Herff Jones maintained its information technology systems ("IT systems"), adequately protected them, and had adequate security safeguards in place, it could have prevented the Data Breach.

63. The totality of industry warnings, awareness of industry best practices, the PCI DSS, and numerous well-documented retail (and other) data breaches alerted Herff Jones to the risk associated with failing to ensure that its IT systems were adequately secured.

64. Herff Jones was aware of the threat of data breaches at large retailers given the numerous recent data breaches that have been prominently covered in the news media, including *inter alia*, breaches involving Target, Home Depot, Wendy's, Chili's, Hy-Vee, Sonic, Wawa, Capital One, Equifax, GameStop, Chipotle, Jason's Deli, Whole Foods, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu. As a result, Herff Jones was manifestly aware that data breaches targeting sensitive Card Information are a real and imminent threat.

65. In addition to the publicly announced data breaches described above (among many others), Herff Jones knew or should have known of additional warnings regarding retail data

breaches, including warnings from the Cybersecurity & Infrastructure Security Agency, a government unit within the Department of Homeland Security, which alerted retailers to the threat of intrusions on July 31, 2014, and issued a guide for retailers on protecting against such a threat, which was updated on August 26, 2014.<sup>8</sup>

66. Despite the fact that Herff Jones was on notice of the very real possibility of consumer data theft associated with its security practices and that Herff Jones knew or should have known about the elementary infirmities associated with its security systems, it still failed to make necessary changes to its security practices and protocols and, thereby, permitted a large breach to occur.

67. Herff Jones, at all times relevant to this action, had a duty to Plaintiffs and class members to: (a) properly secure Card Information submitted to or collected by Herff Jones; (b) protect Card Information using industry standard methods; (c) employ available technology to defend its systems from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiffs and the class, which would naturally result from Card Information theft; and (e) promptly notify customers when Herff Jones became aware of the potential that customers' Card Information may have been compromised.

68. Herff Jones permitted customers' Card Information to be compromised by failing to take reasonable steps against an obvious threat.

69. In addition, leading up to and during the course of the Data Breach, and the investigation that followed, Herff Jones failed to follow the guidelines set forth by the FTC.

---

<sup>8</sup> See Alert (TA14-212A): *Backoff Point-of-Sale Malware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, (July 31, 2014) (revised Sept. 30, 2016), <https://www.us-cert.gov/ncas/alerts/TA14-212A>.

70. Industry experts are clear that a data breach is indicative of data security failures. Indeed, Julie Conroy—research director at the research and advisory firm Aite Group—has identified that: “If your data was stolen through a data breach that means you were somewhere out of compliance” with payment industry data security standards.<sup>9</sup>

71. Had Herff Jones utilized adequate data security and data breach precautions and response protocols, the window of the Data Breach could have been significantly mitigated, and the level of impact could have been reduced, had the breach been permitted to happen at all in the first place.

72. Because payment card data breaches are so common, data security measures are manifestly available to companies that accept and store customer payment information, like Herff Jones. Thus, there is no reasonable basis for Herff Jones’s failure to adequately protect its systems from the Data Breach.

73. As a result of the events detailed herein, Plaintiffs and class members suffered actual, palpable fraud and losses resulting from the Data Breach, including: loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Herff Jones that Plaintiffs and class members would not have made had they known of Herff Jones’s careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information.

---

<sup>9</sup> Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), <http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY>.

74. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges occur and are discovered.

75. Furthermore, the Card Information stolen from Herff Jones can be used to drain debit card-linked bank accounts, make “clone” credit cards, or buy items on certain less-secure websites.

76. To date, and as made clear in its Update, Herff Jones is not taking any real measures to assist affected customers. In the first place, it provided virtually no detail about the Data Breach, leaving victims of the breach in the dark and vulnerable to continued fraud. All that Herff Jones has done in the wake of the breach is create a dedicated support team and phone number for individuals to contact if they believe they have been impacted. Herff Jones’s customers can hardly take comfort in these superficial measures, let alone trust that Herff Jones is now suddenly taking the proper steps to protect class members from fraud.

77. Rather, Herff Jones has shifted the responsibility for the Data Breach to consumers, in lieu of taking real steps to assist its customers in protecting against the fraud to which Herff Jones exposed them.

78. Herff Jones’s failure to adequately protect its customers’ Card Information has resulted in consumers having to undertake various errands (e.g., obtaining credit monitoring, checking credit reports, etc.) that require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of their own money—while Herff Jones is doing nothing to assist those affected by the Data Breach, and withholding important details about the Data Breach as it conducts its investigation.

79. Instead, Herff Jones is putting the burden on the consumer to discover possible fraudulent transactions.

### **CLASS ALLEGATIONS**

80. Plaintiffs bring this action individually and on behalf of the following class pursuant to Federal Rule of Civil Procedure 23:

#### **Nationwide Class**

All individuals in the United States who had their credit or debit card information compromised as a result of the Herff Jones data breach.

81. In the alternative, Plaintiffs brings this action individually and on behalf of the following state subclasses:

#### **New York Class**

All individuals in New York who had their credit or debit card information compromised as a result of the Herff Jones data breach.

#### **Wisconsin Class**

All individuals in Wisconsin who had their credit or debit card information compromised as a result of the Herff Jones data breach.

82. Excluded from the class are Herff Jones, its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change, or expand the definitions of the class based on discovery and further investigation.

83. **Numerosity**: While the precise number of class members has not yet been determined, members of the class are so numerous that their individual joinder is impracticable, as the proposed class appears to include tens of thousands of members who are geographically dispersed.

84. **Typicality**: Plaintiffs' claims are typical of the claims of the class. Plaintiffs and all class members were injured through Herff Jones's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every

other class member because Plaintiffs and each member of the class had their sensitive data and Card Information compromised in the same way by the same conduct by Herff Jones.

85. **Adequacy**: Plaintiffs are adequate representatives of the class because their interests do not conflict with the interests of the class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in class action litigation; and Plaintiffs and their counsel intend to prosecute this action vigorously. The interests of the class will be fairly and adequately protected by Plaintiffs and counsel.

86. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for individual members of the class to effectively redress Herff Jones's wrongdoing. Even if class members could afford such individual litigation, the court system could not withstand it. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

87. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to Plaintiffs and all class members. These questions predominate over the questions affecting individual class members. These common legal and factual questions include, but are not limited to, the following:

- whether Herff Jones engaged in the wrongful conduct alleged herein;

- whether Herff Jones owed duties to Plaintiffs and members of the class to protect their Card Information and to provide timely and accurate notice of the Data Breach, and whether it breached these duties;
- whether Herff Jones violated federal and state laws as a result of the Data Breach;
- whether Herff Jones knew or should have known that its computer and network systems were vulnerable to attacks from hackers and cyber-criminals;
- whether Herff Jones's conduct resulted in or was the proximate cause of the Data Breach, resulting in the theft of customers' Card Information;
- whether Herff Jones wrongfully failed to inform Plaintiffs and members of the class that it did not maintain computer software and other security procedures and precautions sufficient to reasonably safeguard consumers' sensitive financial and personal data;
- whether Herff Jones failed to inform Plaintiffs and class members of the Data Breach in a timely and accurate manner;
- whether Herff Jones continues to breach duties to Plaintiffs and class members;
- whether Herff Jones has sufficiently addressed, remedied, or protected Plaintiffs and class members following the Data Breach and has taken adequate preventive and precautionary measures to ensure the Plaintiffs and class members will not experience further harm;
- whether Plaintiffs and members of the class suffered injury as a proximate result of Herff Jones's conduct or failure to act; and
- whether Plaintiffs and the class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiffs and

the class.

88. Herff Jones has acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the class, thereby making appropriate final injunctive and declaratory relief with respect to the class as a whole.

89. Given that Herff Jones has engaged in a common course of conduct as to Plaintiffs and the class, who have suffered similar or identical injuries and common law and statutory violations are involved, common questions outweigh any potential individual questions.

90. The class is defined in terms of objective characteristics and common transactional facts; namely, the exposure of sensitive Card Information to cyber criminals due to Herff Jones's failure to protect this information, adequately warn the class that it lacked adequate data security measures, and failure to adequately warn that it was breached. Class membership will be readily ascertainable from Herff Jones's business records, and/or from records of third parties.

91. Plaintiffs reserve the right to revise the above class definitions and any of the averments of fact herein based on facts adduced in discovery.

### **COUNT I**

#### **Negligence**

**(On Behalf of Plaintiffs and the Nationwide Class  
or, in the alternative, the New York and Wisconsin Subclasses)**

92. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

93. Herff Jones collected Card Information from Plaintiffs and class members in exchange for its graduation-related goods.

94. Herff Jones owed a duty to Plaintiffs and the class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information in Herff Jones's possession from being compromised by unauthorized persons. This duty included,

among other things, designing, maintaining, and testing Herff Jones's networks and data security systems to ensure that Plaintiffs' and class members' financial and personal information in Herff Jones's possession was adequately protected during the collection of the information and so long as it continues to be stored on Herff Jones's systems.

95. Herff Jones further owed a duty to Plaintiffs and class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

96. Herff Jones owed a duty to Plaintiffs and class members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks—and the personnel responsible for them—adequately protected the financial and personal information of Plaintiffs and class members whose confidential data Herff Jones obtained and maintained.

97. Herff Jones knew, or should have known, of the risks inherent in collecting and storing the financial and personal information of Plaintiffs and class members and of the critical importance of providing adequate security for that information.

98. Herff Jones's conduct created a foreseeable risk of harm to Plaintiffs and members of the class. This conduct included but was not limited to Herff Jones's failure to take the steps to prevent and stop the Data Breach as described herein. Herff Jones's conduct also included its decision to not comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiffs and class members.

99. Herff Jones knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Herff Jones knew or should have

known that hackers would attempt or were attempting to access the personal and financial information in its databases and systems.

100. Herff Jones breached the duties it owed to Plaintiffs and members of the class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the financial and personal information of Plaintiffs and members of the class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiffs and class members.

101. Plaintiffs and class members have suffered non-economic harm as a result of the Data Breach and Defendant's negligence, namely a privacy injury by having their sensitive information disclosed, irrespective of whether or not they subsequently suffered identity fraud. Plaintiffs and class members have also suffered non-economic harm resulting from the time they have spent addressing the fallout of the Data Breach.

102. While one need not be established, a "special relationship" exists between Defendant and the Plaintiffs and class members. Herff Jones entered into a "special relationship" with Plaintiffs and class members by placing their Card Information into Herff Jones's computer system – information that Plaintiffs and class members had been required to provide to Defendant as part of a business transaction. This entrustment of information created a special relationship between the parties, and Defendant had a duty to protect Plaintiffs and class members Card Information.

103. As a direct and proximate result of Herff Jones's negligent conduct, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial.

**COUNT II**  
**Negligence Per Se**  
**(On Behalf of Plaintiffs and the Nationwide Class**  
**or, in the alternative, the New York and Wisconsin Subclasses)**

104. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

105. Pursuant to the FTC Act, 15 U.S.C. § 45, Herff Jones had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and class members' personal information.

106. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Herff Jones, of failing to use reasonable measures to protect Card Information. The FTC publications and orders described above also form part of the basis of Herff Jones's duty to protect Plaintiffs' and class members' sensitive information.

107. Herff Jones violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Card Information and not complying with applicable industry standards, including the PCI DSS, as detailed herein. Herff Jones's conduct was particularly unreasonable given the nature and amount of Card Information it collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers and financial institutions.

108. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the class.

109. Herff Jones had a duty to Plaintiffs and class members to implement and maintain reasonable security procedures and practices to safeguard their Card Information.

110. Herff Jones breached its duties to Plaintiffs and class members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and class members' Card Information.

111. Herff Jones's violation of Section 5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence per se.

112. But for Herff Jones's wrongful and negligent breach of its duties owed to Plaintiffs and class members, they would not have been injured.

113. The injury and harm suffered by Plaintiffs and class members was the reasonably foreseeable result of Herff Jones's breach of its duties. Herff Jones knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and class members to suffer the foreseeable harms associated with the exposure of their Card Information.

114. Had Plaintiffs and class members known that Herff Jones did and does not adequately protect customer Card Information, they would not have made purchases with Herff Jones.

115. As a direct and proximate result of Herff Jones's negligence per se, Plaintiffs and class members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Herff Jones that Plaintiffs and class members would not have made had they known of Herff Jones's careless approach to cyber security; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding payment card limits and balances; harm resulting from damaged credit

scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information, entitling them to damages in an amount to be proven at trial.

**COUNT III**  
**Breach of Implied Contract**  
**(On Behalf of Plaintiffs and the Nationwide Class**  
**or, in the alternative, the New York and Wisconsin Subclasses)**

116. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

117. Plaintiffs and class members who made purchases with Herff Jones had implied contracts with Herff Jones.

118. Specifically, Plaintiffs and class members paid money to Herff Jones and, in connection with those transactions, provided Herff Jones with their Card Information. In exchange, Herff Jones agreed, among other things: (1) to sell or rent graduation caps, gowns, rings, announcements, and other graduation-related goods and services; (2) to take reasonable measures to protect the security and confidentiality of Plaintiffs' and class members' Card Information; and (3) to protect Plaintiffs' and class members' personal information in compliance with federal and state laws and regulations and industry standards.

119. Protection of personal information is a material term of the implied contracts between Plaintiffs and class members, on the one hand, and Herff Jones, on the other hand. Indeed, as set forth, *supra*, Herff Jones recognized the importance of data security and privacy of customers' sensitive financial information vis-à-vis its Privacy Policy. Had Plaintiffs and class members known that Herff Jones would not adequately protect customer Card Information, they would not have made purchases with Herff Jones.

120. Herff Jones did not satisfy its promises and obligations to Plaintiffs and class members under the implied contracts because it did not take reasonable measures to keep their personal information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

121. Herff Jones materially breached its implied contracts with Plaintiffs and class members by failing to implement adequate payment card and Card Information security measures.

122. Plaintiffs and class members fully performed their obligations under their implied contracts with Herff Jones.

123. Herff Jones's failure to satisfy its obligations led directly to the successful intrusion of Herff Jones's computer servers and stored Card Information and led directly to unauthorized parties' access and exfiltration of Plaintiffs' and class members' Card Information.

124. Herff Jones breached these implied contracts as a result of its failure to implement adequate security measures.

125. Also, as a result of Herff Jones's failure to implement adequate security measures, Plaintiffs and class members have suffered actual damages resulting from the theft of their personal information and remain at imminent risk of suffering additional damages in the future.

126. Accordingly, Plaintiffs and class members have been injured as a proximate result of Herff Jones's breaches of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

**COUNT IV**  
**Violations of the New York Deceptive Practices Act**  
**N.Y. Gen. Bus. Law § 349 ("GBL")**  
**(On Behalf of Plaintiff Furcinito and the Nationwide Class,**  
**or, in the alternative, the New York Subclass)**

127. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

128. Plaintiff Furcinito and Class members are “persons” within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(h).

129. Herff Jones is a “person, firm, corporation or association or agent or employee thereof” within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(b).

130. Under GBL Section 349, “[d]eceptive acts or practices in the conduct of any business, trade or commerce” are unlawful.

131. In the course of Herff Jones’s business, it failed to disclose and actively concealed that it does not provide adequate data security and privacy in connection with collecting and maintaining sensitive Card Information as part of transactions with its customers. Defendant did so with the intent to cause Plaintiff and other consumers to rely on this concealment in deciding whether to transact business with Herff Jones.

132. By concealing its known data privacy and the unsecure nature of its payment card transactions, Herff Jones engaged in deceptive acts or practices in violation of GBL § 349.

133. Herff Jones’s deceptive acts or practices were materially misleading. Its conduct was likely to and did deceive reasonable consumers, including Plaintiff, about the true nature of Herff Jones’s data security practices and how it protects Card Information provided to it by consumers.

134. Plaintiff and the Class members reasonably relied on Defendant’s omissions of material facts. Plaintiff and Class members were unaware of, and lacked a reasonable means of discovering, the material facts that Defendant suppressed. Had Plaintiff and Class members known the truth, they would not have shopped with Herff Jones, or would not have paid as much as they did for Herff Jones’s products.

135. Defendant’s actions set forth above occurred in the conduct of trade or commerce.

136. Defendant's conduct concerns widely purchased consumer products and affects the public interest. Defendant's conduct includes unfair and misleading acts or practices that have the capacity to deceive consumers and are harmful to the public at large.

137. Plaintiff and Class members suffered ascertainable loss as a direct and proximate result of Defendant's GBL violations. Among other things, Plaintiff and Class members lost time and money resolving fraudulent charges; lost time and money obtaining protections against future identity theft; suffered financial losses related to the purchases made at Herff Jones that Plaintiff and class members would not have made had they known of Herff Jones's careless approach to cybersecurity; lost control over the value of personal information; suffered unreimbursed losses relating to fraudulent charges; suffered losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; suffered harm resulting from damaged credit scores and information; and suffered other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information. These injuries are the direct and natural consequence of Defendant's material omissions.

138. Plaintiff Furcinito, individually and on behalf of the Class, requests that this Court enter such orders or judgments as may be necessary to enjoin Herff Jones from continuing its unfair and deceptive practices.

139. Under the GBL, Plaintiff and Class members are entitled to recover their actual damages or \$50, whichever is greater. Additionally, because Defendant acted willfully or knowingly, Plaintiff Furcinito and Class members are entitled to recover three times their actual damages. Plaintiff Furcinito also is entitled to reasonable attorneys' fees.

**COUNT V**  
**Violations of the Wisconsin Deceptive Trade Practices Act**  
**Wis. Stat. §§ 100.18, *et seq.* (“WDPTA”)**  
**(On Behalf of Plaintiff Barnicle and the Wisconsin Subclass)**

140. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

141. The WDPTA, §100.18(1) states, in relevant part that no

“firm, corporation or association, . . . with intent to sell, distribute, increase the consumption of . . . any . . . merchandise, . . . service, or anything offered by such person, firm, corporation or association, . . . directly or indirectly, to the public for sale, . . . shall make, publish, disseminate, circulate, or place before the public, . . . in this state, . . . an advertisement, announcement, statement or representation of any kind to the public relating to such . . . sale . . . of such . . . merchandise, . . . [or] service, which advertisement, announcement, statement or representation contains any assertion, representation or statement of fact which is untrue, deceptive or misleading.”

*Id.*

142. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the protection of the Card Information of Plaintiff Barnicle and Wisconsin class members, Herff Jones violated the provisions of § 100.18 of the WDTPA.

143. Herff Jones’s conduct as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to, its omissions concerning customer privacy and that it does not utilize adequate data security measures to protect customers’ sensitive Card Information.

144. Herff Jones’s untrue, deceptive, and misleading omissions concerning its data security materially induced Plaintiff Barnicle and other members of the Wisconsin class to pay more than they otherwise would have paid to Herff Jones had they known of its inadequate data security measures, and caused Plaintiff Barnicle to suffer losses.

145. Herff Jones had a duty to disclose to Plaintiff Barnicle and members of the Wisconsin class that it did not adequately protect their sensitive Card Information, because the

facts were material to Barnicle's and the Wisconsin class members' transactions; because Herff Jones was the party with knowledge of its data security shortcomings; because Herff Jones knew that Barnicle and members of the Wisconsin class were entering transactions under a mistake as to the fact of its data security practices; because that fact was peculiarly and exclusively within Herff Jones's knowledge, and Barnicle and Wisconsin class members could not reasonably be expected to discover it; and on account of the objective circumstances, Plaintiff Barnicle and the members of the Wisconsin class reasonably expected disclosure of the fact that Herff Jones did not protect sensitive Card Information.

146. Due to the Data Breach, Plaintiff and Wisconsin class members have sustained fraud and lost property in the form of their Card Information and have otherwise suffered actual damages. Further, Herff Jones's failure to adopt reasonable practices in protecting and safeguarding the confidential and sensitive financial information of its customers has resulted in Plaintiff Barnicle and Wisconsin class members spending time and money to protect against identity theft. Plaintiff and Wisconsin class members are now at a higher risk of identity theft crimes. This harm sufficiently outweighs any justifications or motives for Herff Jones's practice of collecting and storing confidential and sensitive financial information without the appropriate and reasonable safeguards to protect such information.

147. As a result of Herff Jones's practices, Plaintiff Barnicle and Wisconsin class members have suffered injury-in-fact and have lost money or property. As a result of Herff Jones's failure to adopt, implement, and maintain reasonable security procedures, and the resulting Data Breach, Plaintiff and Wisconsin class members have incurred costs and spent time associated with monitoring and repairing their credit and issues of identity theft.

148. Herff Jones's conduct proximately caused the injuries to Plaintiff Barnicle and the Wisconsin class members and they are entitled to all damages, in addition to costs, interest and fees, including attorneys' fees, as allowed by law.

**COUNT VI**  
**Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.***  
**(On Behalf of Plaintiffs and the Nationwide Class)**

149. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

150. There is an actual controversy between Herff Jones and Plaintiffs concerning, *inter alia*:

- a. Whether Herff Jones owes a duty of care to Plaintiffs and class members with respect to protecting Card Information from unauthorized disclosure;
- b. Whether Herff Jones knew or should have known of its data security shortcomings;
- c. Whether Herff Jones was susceptible to a data breach, and concealed that it was susceptible to a data breach;
- d. Whether Herff Jones engaged in deceptive, unlawful, or unfair acts;
- e. Whether Herff Jones timely and adequately disclosed the Data Breach;
- f. Whether Herff Jones is taking adequate measures to protect customers following the breach;
- g. Whether Plaintiffs and class members sustained damages and the proper measure thereof; and

- h. Whether Herff Jones should be declared financially responsible for notifying class members that card transactions with Herff Jones are susceptible to exposure through data breaches.

151. Pursuant to 28 U.S.C. §§ 2201, the Court may “declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought.”

152. Declaratory relief is intended to minimize “the danger of avoidable loss and unnecessary accrual of damages.” 10B Charles Alan Wright, Arthur R. Miller & Mary Kay Kane, Federal Practice and Procedure § 2751 (3d ed. 1998).

153. Absent being required to change its data security and privacy practices on a forward-looking basis, consumers, including Plaintiffs, will continue to be at risk of harm and susceptible to having their Card Information exposed to criminals by Herff Jones.

154. Accordingly, Plaintiffs seek a declaration that Herff Jones does not comply with its obligations and duties to safeguard customers’ sensitive Card Information, and that Herff Jones must do so going forward, including by taking the following measures:

- a. protect all data collected or received through the course of its business in accordance with federal, state and local laws, and best practices under data security and privacy industry standards;
- b. design, maintain, and test its computer systems to ensure that Card Information in its possession is adequately secured and protected;
- c. disclose any future data breaches in a timely and accurate manner;
- d. engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on

Defendant's systems on a periodic basis and promptly correcting any problems or issues detected by these auditors;

- e. audit, test, and train its security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner;
- f. implement multi-factor authentication requirements;
- g. requiring encryption of all Card Information collected during transactions
- h. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- i. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- j. requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner Card Information no longer necessary for the provision of services;
- k. requiring Defendant to conduct regular computer system scanning and security checks;
- l. requiring Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- m. requiring Defendant to provide multi-year credit monitoring and identity theft repair services to class members.

155. The declaratory relief requested herein will generate common answers that will settle the parties' controversy. There is an economy to resolving these issues as they have the potential to eliminate the need for continued and repeated litigation.

**COUNV VII**  
**Unjust Enrichment**  
**(On Behalf of Plaintiffs and the Nationwide Class**  
**or, in the alternative, the New York and Wisconsin Subclasses)**

156. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

157. This claim is pleaded in the alternative to the above implied contract claim.

158. Plaintiffs and class members conferred a monetary benefit upon Herff Jones in the form of monies paid for the purchase of graduation-related goods and products.

159. Herff Jones appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and class members. Herff Jones also benefited from the receipt of Plaintiffs' and class members' Card Information, as this was utilized by Herff Jones to facilitate payment to it.

160. The monies that Plaintiffs and class members paid to Herff Jones were supposed to be used by Herff Jones, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

161. As a result of Herff Jones's conduct, Plaintiffs and class members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and class members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

162. Under principals of equity and good conscience, Herff Jones should not be permitted to retain the money belonging to Plaintiffs and class members because Herff Jones failed

to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

163. Herff Jones should be compelled to disgorge into a common fund for the benefit of Plaintiffs and class members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

### **PRAYER FOR RELIEF**

Plaintiffs, on behalf of themselves and the class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), and, pursuant to Federal Rule of Civil Procedure 23(g), appoint Plaintiffs as class representative and counsel as class counsel.

B. Award Plaintiffs and the class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement.

C. Award Plaintiffs and the class equitable, injunctive, and declaratory relief as may be appropriate. Plaintiffs, on behalf of the class, seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information, extend credit monitoring services and similar services to protect against all types of identity theft, especially including card theft and fraudulent card charges, and to provide elevated credit monitoring services to minor and elderly class members who are more susceptible to fraud and identity theft.

D. Award Plaintiffs and the class pre-judgment and post-judgment interest to the maximum extent allowable.

- E. Award Plaintiffs and the class reasonable attorneys' fees and costs as allowable.
- F. Award Plaintiffs and the class such other favorable relief as allowable under law or at equity.

Dated: June 11, 2021

Respectfully submitted,

/s/ Richard Shevitz

Irwin B. Levin, No. 8786-49  
Richard E. Shevitz, No. 12007-49  
**COHEN & MALAD, LLP**  
One Indiana Square, Suite 1400  
Indianapolis, IN 46204  
(317) 636-6481  
ilevin@cohenandmalad.com  
rshevitz@cohenandmalad.com

Robert Ahdoot\*

*rahdoot@ahdootwolfson.com*  
**AHDOOT & WOLFSON, PC**  
2600 W. Olive Ave., Suite 500  
Burbank, CA 91505  
Tel: (310) 474-9111  
Fax: (310) 474-8585

Andrew W. Ferich\*

*aferich@ahdootwolfson.com*  
**AHDOOT & WOLFSON, PC**  
201 King of Prussia Road, Suite 650  
Radnor, PA 19087  
Tel: (310) 474-9111  
Fax: (310) 474-8585

*\*pro hac vice to be filed*

*Counsel for Plaintiff and the Proposed Class*